

W. DOUGLAS SPRAGUE (Bar No. 202121)
COVINGTON & BURLING LLP
Salesforce Tower
415 Mission Street, Suite 5400
San Francisco, California 94105-2533
Telephone: (415) 591-6000
Facsimile: (415) 591-6091
Email: dsprague@cov.com

MEGAN A. CROWLEY (admitted *pro hac vice*)
CHLOE GOODWIN (admitted *pro hac vice*)
COVINGTON & BURLING LLP
One City Center
850 Tenth Street, NW
Washington, DC 20001-4956
Telephone: (202) 662-5367
Facsimile: (202) 662-6291
Email: mcrowley@cov.com
cgoodwin@cov.com

Attorneys for Third Party Microsoft Corporation

**UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA
SAN FRANCISCO DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

v.

CIAN BURLEY,

Defendant.

No. 21-CR-00198 EMC

**THIRD PARTY MICROSOFT
CORPORATION'S SUPPLEMENTAL
SUBMISSION IN FURTHER SUPPORT
OF MOTION TO QUASH**

Honorable Edward M. Chen

On May 3, 2023, this Court heard oral argument on Third Party Microsoft Corporation's Motion to Quash Request 5 and part of Request 10 of Defendant's Rule 17(c) subpoena. At the conclusion of the argument, the Court instructed Microsoft to submit a declaration explaining the basis for Microsoft's assertion that someone at Microsoft viewed the images at issue in CyberTip 52016239 before they were sent to NCMEC, considering that Microsoft answered "Yes" to the CyberTip question "Did Reporting [Electronic Service Provider ('ESP')] view entire contents of uploaded file?" Specifically, the Court asked that the declaration include information about how the declarant knows (1) it was Microsoft's policy or practice to answer the foregoing question in the affirmative only when someone manually reviewed the

1 images at issue before they were sent to NCMEC, and (2) the individual who viewed the files complied
2 with Microsoft's policy to manually review the images. *See* Transcript of Proceedings Before the Hon.
3 Edward M. Chen (May 3, 2023) ("Tr.") at 21-22; *see also id.* at 19.

4 In compliance with the Court's instruction, Microsoft hereby submits the Declaration of Alon
5 Brown, Partner Director of the Digital Trust and Safety Team in the Experiences and Devices Division at
6 Microsoft. *See* Ex. 1 (Declaration of Alon Brown). The Declaration explains that all user images shared
7 on Skype which PhotoDNA identifies as containing suspected child sexual exploitation and abuse imagery
8 undergo one of two types of manual review: (1) "double-blind review," in which two analysts
9 independently visually review the image, or (2) "confirm review," in which a single analyst visually
10 reviews the image. *Id.* ¶ 9. The Declaration further explains that, during their training, "analysts are
11 instructed to visually inspect every image they are sent to review," and that once the analyst is shown the
12 image and manually interacts with the review tool, Microsoft's system automatically responds "Yes" to
13 the question "Did Reporting ESP view entire contents of uploaded file?" *Id.* ¶¶ 9, 11-12. The Declaration
14 states that these procedures were in place in 2019. *Id.* ¶ 18. The Declaration further explains that Mr.
15 Brown knows this information based on his personal knowledge, review of Microsoft's records, and
16 discussions with appropriate Microsoft personnel. *Id.* ¶ 1.

17 The Declaration also attaches certain records specific to CyberTip 52016239, which independently
18 confirm that someone at Microsoft manually reviewed the images at issue. The data log entries reflect
19 that the images at issue in CyberTip 52016239 were visually reviewed. Ex. 1 ¶ 15. The entries for each
20 of the four images associated with CyberTip 52016239 reflect that the method of review was "manual,"
21 and that two of the images were subjected to "double-blind" review. *Id.* ¶ 14, Ex. B (Microsoft review
22 log summary). The reference to "double-blind" review means that two individuals at Microsoft separately
23 visually reviewed those two images. Ex. 1 ¶ 15.

24 The information provided in the Declaration far exceeds the information that other courts have
25 found sufficient to establish the scope of an ESP's review in similar cases. *See, e.g., United States v.*
26 *Bohannon*, 2023 WL 2347420, at *1 (N.D. Cal. Mar. 2, 2023); *United States v. Eley*, 2022 WL 181255,
27 at *3 (D. Nev. Jan. 20, 2022); *United States v. Bonds*, 2021 WL 4782270, at *1, *3 (W.D.N.C. Oct. 13,
28 2021). At oral argument, defense counsel argued that *Eley* and *Bonds* are distinguishable from this case

1 because they involved CyberTips issued by Google, which contained an explanation of the meaning of a
2 “Yes” response within the CyberTips themselves. Tr. at 8. In response to questioning from the Court,
3 defense counsel stated, “somebody had to copy and paste” Google’s explanatory language into its
4 CyberTips, and, “somebody who has the personal knowledge to check the ‘yes’ box or the ‘no’ box, is
5 filling out this entire form.” Tr. at 9-10. Moreover, when the Court asked defense counsel whether
6 Google’s policy “is set forth in greater detail in *Eley* than it is in the proposed affidavit here,” defense
7 counsel responded in the affirmative, stating that the Google CyberTip language “is the manual that
8 explain[s] . . . when you are filling out this CyberTip, what does ‘yes’ mean and what does ‘no’ mean.”
9 Tr. at 17. The Court then asked, “you are saying that there is a written instruction to the person filling out
10 the CyberTip, [explaining] exactly what they are supposed to do[?],” to which defense counsel replied
11 “exactly.” *Id.* The Court confirmed defense counsel’s representation, stating “so what you are saying is
12 that the actual instruction in that particular case was set forth [in the CyberTip],” to which defense counsel
13 again replied “exactly.” Tr. at 18.

14 Microsoft has now re-reviewed the *Eley* and *Bonds* decisions, as well as the briefing underlying
15 those decisions and all publicly available supporting documents, including the CyberTips at issue.
16 Microsoft has found no basis in the public records in *Eley* and *Bonds* to support defense counsel’s
17 assertions that (1) the people who viewed the images at issue in those cases (or anyone else with personal
18 knowledge of the review) completed Google’s CyberTips, (2) anyone manually copied and pasted the
19 language explaining the meaning of the “Yes” response into each Google CyberTip, (3) a single person
20 (as opposed to an automated process) manually filled out Google’s CyberTips, or (4) Google’s explanatory
21 language was reflected in any manual or other instruction to the employees who reviewed images
22 associated with CyberTips.

23 Because the attached Declaration and records clearly show that someone at Microsoft manually
24 reviewed each of the images at issue in CyberTip 52016239, Microsoft requests that the Court grant its
25 Motion to Quash Requests 5 and 10 (in part) of Defendant’s subpoena, which seek materials that—at
26 best—would be cumulative of the specific, detailed information Microsoft has submitted in this case.
27 Should Defendant still believe there are any deficiencies in the information Microsoft has agreed to
28

1 produce, Defendant likely will raise them in his forthcoming motion to suppress. But they are not reasons
2 to deny Microsoft's motion to quash Requests 5 and 10 (in part).

3 Dated: May 12, 2023

Respectfully submitted,

4 COVINGTON & BURLING LLP

5 By: /s/ W. Douglas Sprague
6 W. Douglas Sprague

7 *Attorney for Third Party Microsoft Corporation*
8
9
10
11
12
13
14
15
16
17
18
19
20
21
22
23
24
25
26
27
28

Exhibit 1

DECLARATION OF ALON BROWN

1. ***Identity of Declarant.*** My name is Alon Brown and I have been employed by Microsoft since January of 1996. I am currently Partner Director of the Digital Trust and Safety Team in the Experiences and Devices Division at Microsoft. As part of my responsibilities in this role, I am familiar with Microsoft's PhotoDNA technology and Microsoft's processes for reporting images detected on Microsoft's Skype service using PhotoDNA to the National Center for Missing and Exploited Children ("NCMEC"), as required by law, *see* 18 U.S.C. § 2258A. I base this declaration on my personal knowledge, my review of CyberTipline Report 52016239 (the "Report"), Microsoft business records kept in the ordinary course of business, and my discussions with appropriate Microsoft personnel. If called as a sworn witness, I could and would testify competently to the facts stated in this declaration.

2. ***Microsoft's Business Interests in Online Safety.*** Microsoft has a long-standing commitment and legitimate business interest in child online protection. In Microsoft's experience, the direct and indirect costs resulting from the presence of such images on its services can be significant. For example, they can increase the volume of consumer complaints received by Microsoft and, potentially, cause substantial harm to Microsoft's image and reputation in the marketplace. Microsoft believes that its customers are entitled to safer and more secure online experiences that are free of images depicting child sexual abuse. For these reasons, Microsoft devotes resources and develops and deploys technology to protect children online, and invests in research to better understand and combat online child sexual exploitation. Microsoft is also a member of WeProtect, a global alliance of technology companies and international organizations dedicated to ending the sexual exploitation of children online. *See, e.g.,* Courtney Gregoire, *Fighting Child Exploitation as an Industry*, MICROSOFT (June 12, 2020), <https://blogs.microsoft.com/on-the-issues/2020/06/12/fighting-child-exploitation-project-protect>; *Digital Safety Content Report*, MICROSOFT, <https://www.microsoft.com/en-us/corporate-responsibility/digital-safety-content-report> (last visited May 12, 2023).

3. Microsoft has codified its commitment to protecting children online in the “Code of Conduct” provision of the Microsoft Services Agreement (“MSA”), which applies across a wide range of Microsoft services, including Skype, Skype Manager, Skype.com, and Skype in the Classroom. See *Microsoft Services Agreement*, MICROSOFT (effective Aug. 15, 2022), <https://www.microsoft.com/en-us/servicesagreement>. The Code of Conduct sets online community standards and, among other things, prohibits “do[ing] anything illegal” and “engag[ing] in any activity that exploits, harms, or threatens to harm children.” *Id.* ¶ 3. These terms are informed, in part, by Microsoft’s business interests in ensuring its services are not used to proliferate the exploitation and abuse of children.

4. The MSA incorporates the Microsoft Privacy Statement, which describes how Microsoft uses and processes customer data. The Privacy Statement explains “some of our products . . . systematically scan content in an automated manner to identify . . . abusive actions . . . ; and we reserve the right to block delivery of a communication or remove content if it violates our terms.” *Microsoft Privacy Statement*, MICROSOFT (updated Apr. 2023), <https://privacy.microsoft.com/en-us/privacystatement>.

5. **PhotoDNA.** Microsoft enforces the Code of Conduct and Privacy Statement and seeks to fulfill its commitment to ensuring a safe online environment for its users by, among other things, using PhotoDNA. PhotoDNA is an industry-leading image-matching technology developed by Microsoft in collaboration with Dartmouth College that helps Microsoft, along with more than 300 other companies and organizations across the globe, find and remove images of child sexual exploitation and abuse from online services. PhotoDNA compares image “hashes” (unique digital fingerprints) against a database of “hashes” (unique digital fingerprints) of known images of child sexual abuse to identify duplicate images. See generally *PhotoDNA*, MICROSOFT, <https://www.microsoft.com/en-us/photodna> (last visited May 12, 2023). No government agency or law enforcement officer directed or requested that Microsoft create or use PhotoDNA.

6. PhotoDNA uses a mathematical algorithm to create a unique signature—similar to a fingerprint—for each digital image. It does so by adjusting the image to a standard size for processing; converting the image into black and white and breaking the image into sections; calculating a unique number to represent each section; and then placing all those numbers together to create a single code that uniquely represents that image. That code is a unique signature for the digital image, which can be compared with the signatures of other images to find copies of the original illicit image.

7. The technique described in the above paragraph is known as “hashing.” PhotoDNA’s robust hashing differs from other hashing technologies because the PhotoDNA signature is based on the essence of the image and not the specific electronic file containing the image. Therefore, if an image has been resized, recolored, saved in a different file format, or otherwise similarly altered, PhotoDNA can still reliably identify copies of the image when other hashing technologies (that require every file characteristic to be precisely the same) could not.

8. ***Microsoft’s Use of PhotoDNA on Skype.*** Microsoft uses PhotoDNA on several of its consumer services, including Skype. Skype is a telecommunications technology Microsoft acquired in 2011 that allows users to communicate with each other including via messaging. See Skype, <https://www.skype.com/en/features> (last visited May 12, 2023). When a user sends an image via Skype, Microsoft scans the image using PhotoDNA. Microsoft performs these scans to help ensure the safety of Skype (Skype is covered by the MSA, its Code of Conduct, and the Privacy Statement). Specifically, using PhotoDNA on Skype reduces the risk that Microsoft users will be exposed to child sexual exploitation and abuse imagery.

9. All PhotoDNA hashes used in Microsoft’s matching process fall into one of two categories: those that have been previously verified by Microsoft or its agents and those that were provided by Microsoft-approved sources but have yet to be verified by Microsoft or its agents. If an image is shared on Skype and that image’s PhotoDNA hash is found to match a not-yet-verified

PhotoDNA hash provided by a Microsoft-approved source, then the image shared on Skype undergoes "double-blind review" in which it is independently reviewed and classified by two analysts without knowledge of the hash classification that identified the image. In cases of disagreement between those reviews, the image is automatically sent to an escalation process. Such escalated cases are reviewed by two or more additional team members and the team management to make a final determination. If the content is verified as an image of child sexual abuse, thereafter that image's hash becomes a Microsoft Verified Hash. This double-blind review process was designed to mitigate individual bias and increase the quality and consistency of the classification process. If an image is shared on Skype and that image's PhotoDNA hash is found to match a Microsoft verified hash, then the image shared on Skype undergoes a "confirm review" in which the image and the previously verified classification is shown to an analyst for a single, eyes-on review to confirm if the existing classification correctly reflects the content of the image. If, upon reviewing the image, the analyst disagrees with the earlier classification, then the image is automatically sent for additional analyst review as part of a "reclassification" process. In all cases, analysts are instructed to visually inspect every image they are sent to review. They receive these instructions during their training.

10. If Microsoft determines that an image a user has sent via Skype contains child sexual abuse, it takes steps that include (1) removing the image from the service to prevent further exposure and dissemination and protect its customers and the integrity of its services, and (2) filing a CyberTipline Report with NCMEC in compliance with U.S. law. The report may contain basic information about the PhotoDNA match, including the file names and Internet Protocol (IP) address(es) associated with the incident.

11. **CyberTipline Report.** I have reviewed the Report attached as Exhibit A. The Report states that the Reporting Electronic Service Provider ("ESP") was "Microsoft - Online Operations Microsoft Microsoft Skype," and that the peer-to-peer client was "Skype." The Report states "Yes" to

the question “Did Reporting ESP view entire contents of uploaded file?” for each image. This signifies that someone at Microsoft visually reviewed the images at issue before they were sent to NCMEC.

12. The reason I know this to be true is because of my familiarity with Microsoft’s business process for manual review that results in Microsoft answering “Yes” to the question posed. Microsoft does not answer “Yes” as a matter of course in every case, but instead provides this answer only when someone at Microsoft has actually reviewed the contents of the user’s image at issue. Such manual review is conducted close in time to Microsoft’s submission of the CyberTipline Report, which involves providing the “Yes” response to the question posed by the CyberTipline template. The response is automatically generated by the review tool after an analyst has been shown the image on screen and manually interacted with the review tool to specify the image’s classification. Microsoft supplies its responses to the CyberTipline template (thereby populating Section A of the CyberTipline Report) as part of its regularly conducted business activities and as required by law.

13. As the relevant question in Section A of this Report makes clear, Microsoft conducted manual review of the “contents of the uploaded file”—that is, the images that the user uploaded. Microsoft does not maintain any database of reference images, and in the course of conducting manual review, Microsoft does not review any reference images. Nor does Microsoft conduct manual review of any reference hash values.

14. Microsoft’s business records confirm that Microsoft conducted manual review of the images at issue in the Report. Specifically, the record attached as Exhibit B states that the “Process” of review for these images was “Manual.” This means that someone at Microsoft visually reviewed the images at issue before they were sent to NCMEC. The record also indicates that two of the images underwent double-blind review, meaning that two individual analysts separately conducted manual review of those images.

15. My knowledge that someone visually reviewed the images is also based on having examined data extracted from logs created by the tool used to perform these reviews. In so doing, I saw that there were six unique sessions in which the images relating to this CyberTip were reviewed:

- two “double-blind” reviews where two analysts independently reviewed and classified the image without knowledge of the hash classification that identified the image and,
- two “confirm” reviews in which a single analyst reviewed and confirmed the existing classification.

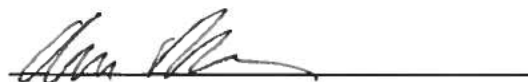
16. Each of the above sessions recorded a completion time, which records when the analyst submitted their classification decision. That means that, in all six cases, an analyst must have manually interacted with the review tool to specify or verify the classification of the image while that image was displayed on screen. In each of those cases, the given image being reviewed was assigned a classification that combined the age (in these cases, pubescent or pre-pubescent) and content (in these cases, a depiction of a “sex act” or “lascivious exhibition of the anus, genitals, or pubic area”) that the analyst identified in the image during their review.

17. The process described in this Declaration was the only automated tool used to identify the images described in this particular CyberTip Report.

18. Based on discussion with appropriate Microsoft personnel, I have been informed that the procedures set forth in paragraphs 9, 10, and 12 are procedures that also were in place in 2019.

19. I declare under penalty of perjury under the laws of the United States of America that the foregoing is true and correct.

Executed on May 12, 2023 in New York, New York.



Alon Brown

Exhibit A



CyberTipline Report 52016239

Priority Level: E
(Report submitted by a registered Electronic Service Provider)

Received by NCMEC on 07-09-2019 02:01:21 UTC

All dates are displayed as MM-DD-YYYY

Except for times provided in Additional Information sections, all time zones are displayed in UTC

Executive Summary

The following is a brief overview of information contained in this CyberTipline report:

Incident Type: Apparent Child Pornography

NCMEC Incident Type is based on NCMEC's review of the report OR a "Hash Match" of one or more uploaded files. NCMEC may not have viewed all uploaded files submitted by the reporting ESP.

NCMEC staff have viewed one or more of the files submitted with this CyberTipline report and have categorized one or more of the files as designated in the Incident Type.

Please see Section C for additional information related to the files that were viewed and categorized by NCMEC.

Total Uploaded Files: 4

The National Center for Missing & Exploited Children (NCMEC) was incorporated in 1984 by child advocates as a private, non-profit 501(c)(3) organization to serve as a national clearinghouse and resource center for families, victims, private organizations, law enforcement, and the public on missing and sexually exploited child issues. To further our mission to help find missing children, reduce child sexual exploitation, and prevent future victimization, NCMEC operates the CyberTipline and Child Victim Identification Program. NCMEC makes information submitted to the CyberTipline and Child Victim Identification Program available to law enforcement and also uses this information to help identify trends and create child safety and prevention messages. As a clearinghouse, NCMEC also works with Electronic Service Providers, law enforcement and the public in a combined effort to reduce online child sexual abuse images. NCMEC performs its programs of work pursuant to its own private mission and independent business operations. NCMEC does not act in the capacity of or under the direction or control of the government or law enforcement agencies. NCMEC does not investigate and cannot verify the accuracy of the information submitted by reporting parties.

CKB-000229

Contents

Section A: Reported Information	1
Reporting Electronic Service Provider (ESP)	1
Company Information	1
Incident Information	1
Peer to Peer	1
Peer to Peer	2
Peer to Peer	2
Peer to Peer	2
Suspect	2
Uploaded File Information	2-4
Section B: Automated Information Added by NCMEC Systems	6
Explanation of Automated Information (in alphabetical order)	6
Further Information on Uploaded Files	6
Geo-Lookup (Suspect)	6
Geo-Lookup (Uploaded Files)	6
Section C: Additional Information Provided by NCMEC	8
NCMEC Note #1	8
Uploaded File Information	8
Section D: Law Enforcement Contact Information	10
San Jose Police Department	10

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
Please treat all information in this Report as confidential.*

Section A: Reported Information

The following information was submitted to the CyberTipline by the Reporting Person or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of the Reporting Person or Reporting ESP.

Reporting Electronic Service Provider (ESP)

Submitter:

Microsoft - Online Operations
Microsoft Microsoft Skype

Business Address:
One Microsoft Way
Redmond, WA 98052 United States

Company Information

U.S. Law Enforcement - Where to serve Legal Process in Criminal Matters

OneDrive, Skype, Xbox, BingImage and other Microsoft Online Services:

Microsoft Corporation
Attn: Custodian of Records
One Microsoft Way
Redmond, WA 98052
Service of Process Only: uslereq@microsoft.com
Inquiries Only: msndcc@microsoft.com

Emergency Requests

Microsoft responds to emergency requests, 24 hours a day, if it relates to the imminent threat of death or serious physical injury as permitted in 18 U.S.C. section 2702(b)(8) and (c)(4). If you have an emergency request, please call the Law Enforcement National Security (LENS) hotline at (425) 722-1299. You may also submit an emergency request via e-mail to lealert@microsoft.com.

Non-U.S. Law Enforcement

Microsoft has established local contacts within your country/region to handle your legal process. If you are not already familiar with your local contact, send an email to globalcc@microsoft.com and you will be directed to the contact handling requests from your country/region. Your local contact will educate you as to what local process must be followed to obtain customer account records. All legal process from non-U.S. law enforcement/prosecutors/courts must be directed to Microsoft Corporation, One Microsoft Way, Redmond, WA 98052 U.S.A. Do not direct your legal process to a local subsidiary of Microsoft.

Incident Information

Incident Type: Child Pornography (possession, manufacture, and distribution)
Incident Time: 07-05-2019 18:13:53 UTC
Description of Incident Time: Incident Time reflects when first image/video in the series was scanned

Peer to Peer

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
Please treat all information in this Report as confidential.*



Peer-to-Peer Client: Skype
IP Address: 68.123.8.91 at 07-05-2019 18:13:53 UTC
Peer to Peer Filenames: 2bf5b62d-9c6f-40ee-abdd-744c59b562f9.jpg

Peer to Peer

Peer-to-Peer Client: Skype
IP Address: 68.123.8.91 at 07-05-2019 18:31:45 UTC
Peer to Peer Filenames: 17a9ae23-8fb4-4c98-8e86-bb732c818fa7.jpg

Peer to Peer

Peer-to-Peer Client: Skype
IP Address: 68.123.8.91 at 07-05-2019 18:35:38 UTC
Peer to Peer Filenames: f0824379-e294-432e-b37f-1cdbcadb7180.jpg

Peer to Peer

Peer-to-Peer Client: Skype
IP Address: 68.123.8.91 at 07-05-2019 18:41:59 UTC
Peer to Peer Filenames: 527789f4-ac96-4f97-8a4a-284cc7be8db7.jpg

Suspect

Screen/User Name: live:ciank111980
IP Address: 68.123.8.91
07-05-2019 18:13:53 UTC
IP Address: 68.123.8.91
07-05-2019 18:31:45 UTC
IP Address: 68.123.8.91
07-05-2019 18:35:38 UTC
IP Address: 68.123.8.91
07-05-2019 18:41:59 UTC
Additional Information: DocumentId: 0-cus-d6-44f9dbeedeb05e4f64bbf5d8aa61adc0
Please provide ScreenName and DocumentId when requesting more information from Microsoft.

Uploaded File Information

Number of uploaded files: 4

Uploaded File Information

Filename: 2bf5b62d-9c6f-40ee-abdd-744c59b562f9.jpg
MD5: 7352f0a58d20e2736fc866cba2832bb8
Submittal ID: b9fc8e1f130e8cc0bd20f2eb54891015
Did Reporting ESP view entire contents of uploaded file? Yes

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
Please treat all information in this Report as confidential.*

CKB-000232



Did Reporting ESP view the EXIF of uploaded file?	(Information Not Provided by Company)
Were entire contents of uploaded file publicly available?	(Information Not Provided by Company)
Image Categorization by ESP: (See Section B for further explanation)	A2
Original Binary Hash of File (PhotoDNA):	50,0,0,26,31,30,10,58,22,153,5,213,101,28,9,237,45,11,8,83,0,14,0,29,89,4,0,71,39,131,88,122,25,236,103,151,243,34,79,108,92,13,54,49,1,18,0,33,124,0,0,102,95,38,25,73,38,255,67,57,255,30,43,37,40,23,2,27,1,22,0,26,145,0,14,48,133,43,16,41,70,249,82,32,219,53,86,21,50,25,15,9,0,26,9,7,115,0,148,4,114,19,104,4,79,217,90,6,184,61,71,4,46,30,91,2,8,13,11,5,4,57,1,71,33,52,16,44,38,45,161,66,41,147,43,67,20,46,2,32,35,15,0,43,48
Original URL Where File was Located:	https://nus1-storage.asm.skype.com:444/v1/objects/0-cus-d6-44f9dbeedeb05e4f64bbf5d8aa61adc0/content/imgpsh

Source Information:

Type	Value	Event	Date/Time
IP Address	68.123.8.91		07-05-2019 18:13:53 UTC

Uploaded File Information

Filename:	f0824379-e294-432e-b37f-1cdbcadb7180.jpg
MD5:	a82d38264e764cb2694581801f55aff4
Submittal ID:	c51eaeae688f59abbc26f8f7ebc3aa1
Did Reporting ESP view entire contents of uploaded file?	Yes
Did Reporting ESP view the EXIF of uploaded file?	(Information Not Provided by Company)
Were entire contents of uploaded file publicly available?	(Information Not Provided by Company)
Image Categorization by ESP: (See Section B for further explanation)	B2
Original Binary Hash of File (PhotoDNA):	32,85,58,81,46,32,35,62,56,47,37,69,61,137,124,59,41,141,73,116,149,4,1,34,154,85,55,96,44,73,150,144,79,93,60,131,94,105,93,126,120,21,158,212,18,197,57,174,31,95,46,72,41,51,129,70,39,113,46,103,55,71,129,9,1,89,125,94,75,62,88,148,107,74,57,39,49,73,31,95,34,47,93,52,44,59,48,121,58,62,126,69,52,60,56,84,94,97,95,60,74,44,49,143,51,62,146,53,59,65,51,88,98,17,81,72,86,28,72,113,118,57,14,7,12,9,17,99,45,33,127,43,63,54,50,82,33,147,74,43,13,118,7,17,24,9
Original URL Where File was Located:	https://nus1-storage.asm.skype.com:444/v1/objects/0-cus-d10-24604fa047f70d6d7f92583667dd66d8/content/imgpsh

Source Information:

Type	Value	Event	Date/Time
IP Address	68.123.8.91		07-05-2019 18:35:38 UTC

Uploaded File Information

Filename:	17a9ae23-8fb4-4c98-8e86-bb732c818fa7.jpg
MD5:	8d293bc6aaf098ba783be853dbe6c0ba
Submittal ID:	d94a67759c4bf03e20ff02e79cc44e60

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
Please treat all information in this Report as confidential.*



Did Reporting ESP view entire contents of uploaded file? Yes
Did Reporting ESP view the EXIF of uploaded file? (Information Not Provided by Company)
Were entire contents of uploaded file publicly available? (Information Not Provided by Company)
Image Categorization by ESP: B2
(See Section B for further explanation)
Original Binary Hash of File (PhotoDNA): 42,41,128,11,114,27,238,30,46,48,73,77,54,17,61,45,24,76,76,37,44,161,54,119,53,44,15,121,107,46,21,177,89,69,38,97,91,44,40,53,26,134,17,139,19,187,19,140,19,60,12,79,107,17,32,114,103,30,25,108,75,75,9,144,2,149,31,157,7,78,39,78,15,82,14,113,162,14,48,124,92,105,30,100,102,110,29,173,6,121,27,142,10,93,44,118,63,57,43,42,136,15,75,46,78,113,109,100,99,88,139,64,8,110,54,18,25,41,39,22,77,47,36,124,151,15,43,113,79,63,92,146,81,79,52,146,16,138,52,24,24,53,12,50
Original URL Where File was Located: <https://nus1-storage.asm.skype.com:444/v1/objects/0-cus-d5-d99abad216610b9d8c0fa759acc364e0/content/imgpsh>

Source Information:

Type	Value	Event	Date/Time
IP Address	68.123.8.91		07-05-2019 18:31:45 UTC

Uploaded File Information

Filename: 527789f4-ac96-4f97-8a4a-284cc7be8db7.jpg
MD5: 0b4c1d2bc6e858affe39aae81989c9aa
Submittal ID: 7b8651a82b379da9057581c80e92416f
Did Reporting ESP view entire contents of uploaded file? Yes
Did Reporting ESP view the EXIF of uploaded file? (Information Not Provided by Company)
Were entire contents of uploaded file publicly available? (Information Not Provided by Company)
Image Categorization by ESP: B1
(See Section B for further explanation)
Original Binary Hash of File (PhotoDNA): 136,162,171,78,174,133,173,68,81,68,195,84,52,81,178,57,79,110,193,49,109,94,166,32,112,162,105,101,140,88,139,74,104,120,98,95,119,67,79,81,85,133,116,88,114,98,107,65,108,81,135,74,70,62,95,36,54,61,113,53,74,65,112,53,49,58,98,58,59,48,82,39,57,51,28,90,46,46,56,57,30,77,30,88,51,58,16,97,62,45,34,106,75,57,39,84,77,51,50,72,54,45,36,102,32,64,32,56,47,41,60,44,53,48,45,46,99,28,94,71,79,27,43,39,50,70,81,37,42,72,40,65,62,36,47,56,41,40,51,34,75,41,28,111
Original URL Where File was Located: <https://nus1-storage.asm.skype.com:444/v1/objects/0-cus-d9-e983dc91be69eb630b9f02d200842093/content/imgpsh>

Source Information:

Type	Value	Event	Date/Time
IP Address	68.123.8.91		07-05-2019 18:41:59 UTC

This concludes Section A. All of the information in this section was submitted electronically to the CyberTipline by the Reporting Person, NCMEC Call Center or Reporting ESP. The information appearing in Section A is information received in the original submission. The reporting of information in Section A, other than the "Incident Type" and "Incident Time," is voluntary and undertaken at the initiative of

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
Please treat all information in this Report as confidential.*

the Reporting Person or Reporting ESP.

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
Please treat all information in this Report as confidential.*

CKB-000235

PROTECTED INFORMATION – SUBJECT TO PROTECTIVE ORDER

Section B: Automated Information Added by NCMEC Systems

Upon receipt of a CyberTipline report, NCMEC Systems may conduct automated processes on the information submitted in Section A. The information found in Section B of this CyberTipline Report has been automatically generated by NCMEC Systems. If the CyberTipline Report was submitted by a member of the public, Section B will be blank.

Explanation of Automated Information (in alphabetical order)

Geo-Lookup: When a Reporting ESP voluntarily reports an IP address for the "Suspect," NCMEC Systems will geographically resolve the IP address via a publicly-available online query. The results of this lookup are displayed.

Geolocation data is approximate and may not display a user's exact location. Please be aware that the geolocation information provided is not exact but is providing a reliable estimate of location based on IP address(es) voluntarily provided by the reporting ESP.

Further Information on Uploaded Files

Number of uploaded files in each categorization category:

A2: 1
B1: 1
B2: 2

The following categorization system was created by various ESPs in January 2014:

	Content Ranking	1	2
A	Prepubescent Minor	A1	A2
B	Pubescent Minor	B1	B2

Rank	Term	Definition
1	Sex Act	Any image of sexually explicit conduct (actual or simulated sexual intercourse including genital-genital, oral-genital, anal-genital, or oral-anal whether between person of the same or opposite sex), bestiality, masturbation, sadistic or masochistic abuse, degradation, or any such depiction that lacks serious literary, artistic, political, or scientific value.
2	Lascivious Exhibition	Any image depicting nudity and one or more of: restraint, sexually suggestive poses, focus on genitals, inappropriate touching, adult arousal, spreading of limbs or genitals, and such depiction lacks serious literary, artistic, political, or scientific value.

Geo-Lookup (Suspect)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
68.123.8.91	US	CA	Santa Rosa	San Francisco-Oakland-San Jose	95401		38.4426 / -122.7547	AT&T Internet Services / AT&T Internet Services

This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission. Please treat all information in this Report as confidential.



Geo-Lookup (Uploaded Files)

IP Address	Country	Region	City	Metro Area	Postal Code	Area Code	Lat/Long	ISP/Org
68.123.8.91	US	CA	Santa Rosa	San Francisco-Oakland-San Jose	95401		38.4426/ - 122.7547	AT&T Internet Services/ AT&T Internet Services

This concludes Section B

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
Please treat all information in this Report as confidential.*

CKB-000237

Section C: Additional Information Provided by NCMEC

Section C contains information collected by NCMEC staff based on the information electronically submitted by the Reporting Person, NCMEC Call Center or Reporting ESP. Section C may contain a variety of additional information, including data gathered from queries on publicly-available, open-source websites. Any queries conducted by NCMEC staff will be documented and any query results will be saved to the electronic filing system when possible. The CyberTipline cannot confirm the accuracy of information found in public records or whether the results are affiliated with any parties relating to this report.

NCMEC Priority Level: E (Report submitted by a registered Electronic Service Provider)
 NCMEC Classification*: Apparent Child Pornography
 International Country: United States
 NCMEC Date Processed: 08-07-2019 20:00:39 UTC
 Made Available to Law Enforcement by NCMEC: Yes

NCMEC Classification is based on NCMEC's review of the report OR a "Hash Match" of one or more uploaded files. NCMEC may not have viewed all uploaded files submitted by the reporting ESP.

NCMEC Note #1

ECD-SEV 08-07-2019 20:00:39 UTC

I reviewed the uploaded files and found what appears to be CHILD PORNOGRAPHY.

=====

CT/TA queries for the following yielded negative or irrelevant results:

68.123.8.91
 ciank111980

=====

Spokeo, Google, Instagram, Twitter, and Kik for ciank111980 returned negative results

=====

Based on the reported IP address, I have sent this report to the San Jose ICAC

Uploaded File Information

Files Viewed by NCMEC:

NCMEC staff have viewed the following uploaded files which had not been previously viewed and categorized by NCMEC at the time this report was generated.

Filename	Files Viewed by NCMEC	MD5
2bf5b62d-9c6f-40ee-abdd-744c59b562f9.jpg		7352f0a58d20e2736fc866cba2832bb8
f0824379-e294-432e-b37f-1cdbcadb7180.jpg		a82d38264e764cb2694581801f55aff4
17a9ae23-8fb4-4c98-8e86-bb732c818fa7.jpg		8d293bc6aaf098ba783be853dbe6c0ba

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
 Please treat all information in this Report as confidential.*



Files Viewed by NCMEC

Filename	MD5
527789f4-ac96-4f97-8a4a-284cc7be8db7.jpg	0b4c1d2bc6e858affe39aae81989c9aa

This concludes Section C

If you need further information regarding the contents of this Report, please contact the CyberTipline at null or 1-877-446-2632, ext. 6702.

For more information regarding images containing identified child victims, please contact the Child Victim Identification Program (CVIP) at cvip@ncmec.org.

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
Please treat all information in this Report as confidential.*

Section D: Law Enforcement Contact Information

The report was made available to the Law Enforcement Agency listed below.

San Jose Police Department

Investigator:

Assigned Officer:	Access VPN
Title:	Det. Christian Mendoza
City/State:	San Jose, CA
Country:	United States
Phone Number:	408-896-3079
Email Address:	christian.mendoza@sanjoseca.gov,jose.montoya@sanjoseca.gov,michael.ogrady@sanjoseca.gov,sean.pierce@sanjoseca.gov

Time/Date was made available: 08-07-2019 20:00:39 UTC

This concludes Section D

This concludes CyberTipline Report 52016239

*This Report is provided solely for informational purposes pursuant to NCMEC's nonprofit mission.
Please treat all information in this Report as confidential.*

CKB-000240

Exhibit B

MSA PUID ⓘ

All

NCMEC Report Id

52016239

Show Export
View

NCMEC Report ID	ScanDateTime	NCMEC Report Date	MSA PUID	Tenant Name	Classification	Review Complete Date	Process	Sentry ID	Queue
52016239	7/5/2019 6:13:53 PM	7/9/2019	3400110ba7fd7	Skype	A2	7/8/2019	Manual	00003ef9-0000-00c9-a541-51aa7401d708	Confirm
52016239	7/5/2019 6:31:45 PM	7/9/2019	3400110ba7fd7	Skype	B2	7/8/2019	Manual	00003f2a-0000-00ea-645f-283e7701d708	Confirm
52016239	7/5/2019 6:35:38 PM	7/9/2019	3400110ba7fd7	Skype	B2	7/8/2019	Manual	00000a40-0000-00f0-0d34-929e7701d708	Double-Blind FTE Only
52016239	7/5/2019 6:35:38 PM	7/9/2019	3400110ba7fd7	Skype	B2	7/8/2019	Manual	00000a46-0000-00e6-9dde-439e7701d708	Double-Blind
52016239	7/5/2019 6:41:59 PM	7/9/2019	3400110ba7fd7	Skype	B1	7/8/2019	Manual	00000a44-0000-0054-bb1f-0f808401d708	Double-Blind
52016239	7/5/2019 6:41:59 PM	7/9/2019	3400110ba7fd7	Skype	B1	7/8/2019	Manual	00000a44-0000-0064-c809-18808401d708	Double-Blind FTE Only

Exhibit 2

IN THE UNITED STATES DISTRICT COURT
 FOR THE NORTHERN DISTRICT OF CALIFORNIA
 SAN FRANCISCO DIVISION

UNITED STATES OF AMERICA,)	CR-21-00198-EMC
)	
PLAINTIFF,)	SAN JOSE, CALIFORNIA
)	
VS.)	MAY 3, 2023
)	
CIAN BURLEY,)	PAGES 1-25
)	
DEFENDANT)	
)	
)	

TRANSCRIPT OF PROCEEDINGS
 BEFORE THE HONORABLE EDWARD M. CHEN
 UNITED STATES DISTRICT JUDGE

A P P E A R A N C E S

FOR THE GOVERNMENT: **BY: EMILY DAHLKE**
 UNITED STATES ATTORNEY'S OFFICE
 450 GOLDEN GATE AVENUE
 SAN FRANCISCO, CA 94102

FOR THE DEFENDANT: **BY: GABRIELA BISCHOF**
 FEDERAL PUBLIC DEFENDER
 450 GOLDEN GATE AVE
 ROOM 19-6884, BOX 36106
 SAN FRANCISCO, CA 94102

APPEARANCES CONTINUED ON NEXT PAGE

OFFICIAL COURT REPORTER: SUMMER FISHER, CSR, CRR
 CERTIFICATE NUMBER 13185

PROCEEDINGS RECORDED BY MECHANICAL STENOGRAPHY
 TRANSCRIPT PRODUCED WITH COMPUTER

APPEARANCES CONTINUED:

FOR THIRD PARTY:
MICROSOFT

BY: WILLIAM DOUGLAS SPRAGUE
COVINGTON & BURLING LLP
415 MISSION STREET, SUITE 5400
SAN FRANCISCO, CA 94105

1 NORMALLY YOU CAN'T USE SUBPOENAS JUST TO FIND IMPEACHING
2 EVIDENCE, I MEAN, IT'S GOT TO HAVE SOME OTHER USE TO IT; WHY
3 ISN'T THAT ENOUGH? THERE WAS A SPECIFIC AFFIRMATION HERE, WHY
4 DO WE NEED TO GET BEYOND THAT?

5 MS. BISCHOF: WELL, YOUR HONOR, I THINK THERE'S A LOT
6 TO UNPACK THERE.

7 I MEAN, I THINK FIRST OF ALL, MICROSOFT'S RELIANCE ON ELEY
8 AND BONDS IS MISPLACED, IT ACTUALLY SUPPORTS OUR POSITION. IN
9 ELEY AND BONDS, THOSE CYBER TIPS, THEY WERE SUBMITTED BY
10 GOOGLE, AND UNDERNEATH THE COMPANY INFORMATION, WHICH IS A
11 SEPARATE SECTION OF THE CYBER TIP, IT SAYS, "WHEN GOOGLE
12 RESPONDS YES, IT MEANS THE CONTENTS OF THE FILE REPORTED WERE
13 VIEWED BY A PERSON CONCURRENTLY TO OR IMMEDIATELY PRECEDING THE
14 SENDING OF THE CYBER TIP," AND IT ALSO EXPLAINS WHAT IT MEANS
15 WHEN GOOGLE RESPONDS "NO."

16 AND SO WHAT THE COURTS FOUND IN THOSE CASES, IS THAT
17 WITHIN THE CYBER TIP ITSELF, THERE WAS SUFFICIENT EVIDENCE,
18 THERE WAS COMPETENT EVIDENCE, THERE WAS RELIABLE EVIDENCE THAT,
19 IN FACT, THESE WERE THE THINGS THAT HAVE HAPPENED IN THESE
20 PARTICULAR CASES.

21 WHAT MICROSOFT IS SAYING THAT THEY WANT TO SUBSTITUTE THE
22 DECLARATION OF SOMEONE WITH NO PERSONAL KNOWLEDGE AS TO WHAT
23 HAPPENED WITH BUSINESS PRACTICES THAT THEY ARE NOT PLANNING TO
24 ELABORATE ON, AND THAT DON'T SET FORTH HOW THOSE BUSINESS
25 PRACTICES WERE COMMUNICATED TO THE PERSON WHO WOULD HAVE BEEN

1 FILLING OUT THE CYBER TIP.

2 SO WHEN YOU LOOK AT ELEY AND BONDS, WHAT YOU REALLY HAVE
3 IS, WITHIN THE DOCUMENT ITSELF, SOMEBODY HAD TO COPY AND PASTE
4 AND SAY, THIS IS WHAT IT MEANS WHEN WE CHECK THE BOX "YES,"
5 THIS IS WHAT IT MEANS WHEN WE CHECK THE BOX "NO," AND INHERENT
6 IN THAT CYBER TIP QUESTION OF, YOU KNOW, DID THE REPORTING ESP
7 VIEW THE ENTIRE CONTENTS OF THE UPLOADED FILE --

8 THE COURT: WHY WASN'T ELEY -- IT WASN'T AS IF THE
9 PERSON WHO ACTUALLY REVIEWED IT SAID, I DECLARE UNDER PENALTY
10 OF PERJURY ON SUCH AND SUCH DATE, I ACTUALLY LOOKED AT THIS
11 STUFF. IT'S STILL IN THE NATURE OF, THIS IS SORT OF OUR
12 PROCESS, IN A WAY. YES, IT MEANS -- WHEN IT SAYS, WAS
13 REVIEWED, IT MEANS "THAT THE CONTENTS OF THE FILE REPORTED WERE
14 VIEWED BY A PERSON CONCURRENTLY TO OR IMMEDIATELY PRECEDING."

15 THAT'S A GENERALIZED STATEMENT OF POLICY, RIGHT? HOW IS
16 THAT ANY DIFFERENT FROM WHAT WE HAVE HERE?

17 MS. BISCHOF: BECAUSE IT'S WITHIN THE CYBER TIP,
18 ITSELF.

19 THE COURT: WHY DOES THAT MATTER?

20 MS. BISCHOF: BECAUSE IT MEANS THAT THE PERSON WHO
21 FILLED IT OUT HAD TO INPUT THAT INFORMATION, WHICH MEANS THAT
22 THEY WERE --

23 THE COURT: BUT WHEN THE PERSON IS TALKING ABOUT
24 PROCESS, IS THERE ANY INDICATION IN ELEY THAT THE PERSON WHO
25 ACTUALLY DID THE VIEWING WAS THE ONE WHO FILLED OUT THE CYBER

1 TIP?

2 MS. BISCHOF: I MEAN, PRESUMABLY, THE PERSON WHO DOES
3 THE VIEWING IS THE ONE WHO FILLED OUT THE CYBER TIP.

4 THE COURT: DID IT SAY THAT? DID IT SAY, I'M THE ONE
5 WHO FILLED IT OUT, AND I ATTEST AND I VIEWED IT?

6 MS. BISCHOF: IT DOESN'T HAVE AN ATTESTATION, BUT
7 WHAT WE ARE TALKING ABOUT IS SOMEBODY WHO HAS THE PERSONAL
8 KNOWLEDGE TO CHECK THE "YES" BOX OR THE "NO" BOX, IS FILLING
9 OUT THIS ENTIRE FORM.

10 AND SO WHEN THE COURTS ARE LOOKING AT THAT, THEY ARE
11 SAYING OKAY, WITHIN THIS FORM, THERE ARE INTERNAL INDICATIONS
12 THAT THIS IS RELIABLE.

13 AND I THINK WHAT THAT ALSO SORT OF GOES TO UNPACK, IS THE
14 COURT'S QUESTION ABOUT, WELL, IS THIS JUST FOR IMPEACHMENT?
15 AND I THINK IT'S ABSOLUTELY NOT JUST FOR IMPEACHMENT. AND
16 THAT'S THE ISSUE. IT'S WHETHER THE GOVERNMENT -- EXCUSE ME --
17 WELL, WHAT WILL BE FOR THE GOVERNMENT, THIS DECLARATION,
18 WHETHER THAT'S COMPETENT EVIDENCE OR SUFFICIENT EVIDENCE FOR
19 THE GOVERNMENT TO MEET ITS BURDEN.

20 BECAUSE HERE, THE BURDEN IS ON THE GOVERNMENT TO SHOW THAT
21 THE PRIVATE SEARCH EXCEPTION APPLIES. SO PUTTING IN A
22 DECLARATION FROM SOMEONE WITH NO PERSONAL KNOWLEDGE OF THE
23 PARTICULAR INCIDENT, WHICH DOESN'T CONVEY HOW THE PERSON
24 FILLING OUT THIS FORM WAS MADE AWARE OF WHAT THESE BUSINESS
25 PRACTICES ALLEGEDLY WERE, WHICH AREN'T NECESSARILY EXPOUNDED

1 STONE, IT SAYS EXACTLY WHAT IT MEANS.

2 AND I DON'T THINK ANY OF THOSE --

3 THE COURT: IS THE POLICY -- THE COMPANY POLICY,
4 REMIND ME, IS IT SET FORTH IN GREATER DETAIL IN ELEY THAN IT IS
5 IN THE PROPOSED AFFIDAVIT HERE?

6 MS. BISCHOF: YES.

7 THE COURT: IN WHAT WAY?

8 MS. BISCHOF: I MEAN, I THINK THAT IT'S -- SO IN BOTH
9 ELEY AND BONDS, WHICH I THINK IS RELEVANT, IT'S THE SAME.

10 AND IT IS THE WRITTEN -- IT'S BASICALLY EXACTLY WHAT WE
11 ARE SEEKING IN THIS CASE, WHICH IS THE MANUAL THAT EXPLAIN THE
12 PORTION THAT SAYS WHEN YOU ARE FILLING OUT THIS CYBER TIP, WHAT
13 DOES "YES" MEAN AND WHAT DOES 'NO' MEAN.

14 AND IT SAYS IT RIGHT THERE IN THERE. WHEN GOOGLE RESPONDS
15 "YES," IT MEANS THE CONTENTS OF THE FILE REPORTED WERE VIEWED
16 BY A PERSON --

17 THE COURT: YOU ARE SAYING THAT THERE IS A WRITTEN
18 INSTRUCTION TO THE PERSON FILLING OUT THE CYBER TIP, EXACTLY
19 WHAT THEY ARE SUPPOSED TO DO.

20 MS. BISCHOF: EXACTLY.

21 THE COURT: ALL RIGHT. SO WHERE HERE, THERE IS NO
22 SUCH WRITTEN INSTRUCTION.

23 MS. BISCHOF: EXACTLY. AND WHAT MICROSOFT WANTS TO
24 SUBMIT IS THE UNDERSTANDING OF SOMEBODY WITH NO PERSONAL
25 KNOWLEDGE ABOUT THIS PARTICULAR CYBER TIP WITHOUT RELATING IT

1 BACK TO --

2 THE COURT: ALL RIGHT.

3 SO WHAT YOU ARE SAYING IS THAT THE ACTUAL INSTRUCTION IN
4 THAT PARTICULAR CASE WAS SET FORTH.

5 MS. BISCHOF: EXACTLY.

6 THE COURT: THE COURT COULD SEE THAT THE PERSON WHO
7 FILLED IT OUT SAW THE INSTRUCTION; WHEREAS HERE, WE JUST SEE
8 THE RESULT AND THEN WE HAVE AN AFTER-~~THE-FACT~~ STATEMENT THAT
9 WELL, IT IS OUR POLICY, BUT WE DON'T KNOW EXACTLY WHAT THAT
10 PERSON SAW.

11 MS. BISCHOF: OR WHAT THE POLICY WAS AT THE TIME.

12 THE COURT: ALL RIGHT.

13 SO THE LOOP WAS CLOSED IN ELEY AND BONDS, BUT NOT SO
14 DEFINITELY CLOSED HERE.

15 MS. BISCHOF: EXACTLY.

16 THE COURT: ALL RIGHT.

17 SO WHAT'S WRONG WITH THAT, MR. SPRAGUE?

18 MR. SPRAGUE: I DON'T KNOW THAT THAT'S ACCURATE,
19 YOUR HONOR.

20 I DON'T KNOW WHAT COUNSEL IS RELYING ON TO SAY THAT THE
21 PERSON FILLED OUT THAT, WHO REVIEWED THE IMAGES, FILLED OUT
22 THAT FORM, AND THAT'S SETTING FORTH THE POLICY THAT THAT PERSON
23 IS SAYING, I'M UNDERSTANDING AND FILLING THIS OUT.

24 I WOULD HAVE TO GO BACK INTO PACER AND FIND THE
25 ATTACHMENTS, AND IF COUNSEL HAS DONE THAT, THEN THEY MIGHT HAVE

1 A BASIS TO SAY WHAT SHE JUST SAID. I HAVEN'T LOOKED AT THAT.
2 I'VE READ THE CASE. OTHERWISE, I THINK THAT'S SPECULATION.

3 AND WHAT IS IN THE CASE IS THAT IT'S FINE FOR THIS PERSON
4 TO REMAIN UNIDENTIFIED. SO I DON'T KNOW THAT THAT PERSON IS
5 FILLING IT OUT, I DON'T KNOW IF THEY ARE ACKNOWLEDGING WHAT
6 THIS POLICY IS.

7 I WOULD ALSO SAY ONE STEP FURTHER, MICROSOFT, IN THIS
8 CASE, IS GOING TO SUBMIT AND HAS REPEATEDLY OFFERED TO SUBMIT A
9 SWORN DECLARATION ON THIS POINT, EXACTLY THAT LANGUAGE THERE IN
10 THE GOOGLE MATTER, WHICH IS, WHEN WE FILL THIS OUT TO SAY WE
11 HAVE REVIEWED IT, HERE'S WHAT IT MEANS.

12 THE COURT: WILL THEY HAVE ANY MORE DETAIL, LIKE WHY
13 WE KNOW IT MEANS WHAT IT MEANS? BECAUSE RIGHT NOW, IT'S RATHER
14 CONCLUSORY. AND THE ONE THAT WAS SUBMITTED BY MR. DAVIS IS
15 RATHER CONCLUSORY. IN FACT, IT ONLY SAYS, THIS SIGNIFIES,
16 WHATEVER THAT MEANS THAT, SOMEONE HAS REVIEWED THE IMAGE. IT
17 DOESN'T SAY HOW WE KNOW THIS.

18 FOR INSTANCE, IT DOESN'T SAY, AND HERE'S WHY I KNOW THIS,
19 BECAUSE WE -- THEY ARE INSTRUCTED, THERE'S A SUPPLEMENTARY MEMO
20 THAT GOES OUT EVERY TIME YOU GET ONE OF THESE THINGS, OR WHEN
21 THEY ARE HIRED ON TO LOOK AT THIS, WE ARE TOLD, THEY ARE TOLD
22 X, Y AND Z. HOW DO WE KNOW THAT?

23 MR. SPRAGUE: IN THE FORM THAT WE'VE SEEN FROM THE
24 DRAFT, OR THE EXAMPLE RATHER, ATTACHED TO THE OPPOSITION, IT
25 DISCUSSES THE BUSINESS PRACTICE.

1 THE COURT: WELL --

2 MR. SPRAGUE: IT DOESN'T HAVE WHAT YOUR HONOR HAS
3 SAID --

4 THE COURT: IT'S CONCLUSORY TO SAY IT'S BUSINESS
5 PRACTICE, WHATEVER THAT MEANS. AND THE EARLIER ONE JUST SAYS
6 "SIGNIFIES," WHATEVER THAT MEANS.

7 MR. SPRAGUE: YEAH. WELL, WE COULD SEE HOW DETAILED
8 WE COULD MAKE THAT, WE COULD FLESH IT OUT IN THIS MATTER FOR
9 WHAT THE BUSINESS PRACTICE IS BASED ON AND HOW THEY HAVE THAT
10 KNOWLEDGE. BUT I DO NOT --

11 THE COURT: MAYBE WE OUGHT TO DO THAT. MAYBE I OUGHT
12 TO SEE -- GET AS SPECIFIC AS YOU CAN, AND IT'S GOING TO BE A
13 DECLARATION UNDER OATH. AND THEN THE ONLY REASON WHY
14 MS. BISCHOF WOULD SAY, IS THAT WELL, THIS PERSON IS LYING, THIS
15 PERSON IS NOT TELLING THE TRUTH.

16 IN OTHER WORDS, IF IT'S SPECIFIC -- SHE HAS AN ARGUMENT
17 RIGHT NOW THAT IT'S NOT VERY SPECIFIC. BUT IF YOU BECOME
18 SPECIFIC, THEN THE ONLY REASON SHE WOULD HAVE FOR RULE 17
19 SUBPOENA IS SAYING, WELL, I DO NOT BELIEVE THIS PERSON -- I
20 THINK THERE'S MORE HOLES IN THIS POLICY THAN THIS PERSON
21 SUGGESTS, OR IT'S NOT AS AIR TIGHT AS THEY SUGGEST.

22 THEN WE GET INTO THIS QUESTION, WELL, CAN YOU USE RULE 17
23 SUBPOENAS, THEN IT BEGINS TO LOOK MORE LIKE IMPEACHMENT.

24 MR. SPRAGUE: WELL, AND I WOULD SAY THAT WOULD BE
25 BELTS AND SUSPENDERS, TO USE ONE PHRASE, YOUR HONOR, CERTAINLY

1 POSSIBLY SOMETHING WE COULD LOOK INTO ON OUR END.

2 I WOULD GO BACK TO THAT I DON'T THINK WILSON REQUIRES IT
3 OR THE CASES DEALING IN THE POST-WILSON CONTEXT OF BOHANNON,
4 ELEY, AND BONDS, HAD THAT INFORMATION, AND THEY RELIED ON MUCH
5 LESS THAN THAT. NO DECLARATION AT ALL, FOR EXAMPLE. IN
6 UPHOLDING THE DENIAL --

7 THE COURT: LET'S DO THIS, I MEAN, MS. BISCHOF IS
8 RIGHT, THERE'S NOT A WHOLE LOT OF LAW, IT'S 2021, YOU GOT THREE
9 CASES, I DON'T KNOW WHERE IT'S GOING TO END UP.

10 IT DOES RAISE AN INTERESTING QUESTION IN SORT OF THE IPSE
11 DIXIT ASSERTION BY THE THIRD PARTY TO SORT OF LOCK DOWN THAT
12 ISSUE. AND ONE COULD ARGUE WELL, IT'S SUCH A CRITICAL ISSUE,
13 YOU KNOW, FROM THE DEFENDANT'S PERSPECTIVE, THAT SHOULD BE THE
14 CASE.

15 ON THE OTHER HAND, YOU KNOW, RULE 17 IS NOT MEANT TO BE A
16 GENERAL DISCOVERY DEVICE, THIS IS NOT CIVIL DISCOVERY, AND
17 SO -- BUT WHAT I WOULD LIKE TO DO IS TO HAVE MICROSOFT PREPARE,
18 WELL, WHY NOT JUST SUBMIT A DECLARATION? I MEAN, JUST DO IT IN
19 A DECLARATION FORM, NOT JUST SAY, HERE'S THE DECLARATION, JUST
20 SUBMIT THE DECLARATION WITH AS MUCH SPECIFICITY AS POSSIBLE.

21 YOU KNOW WHAT THE ISSUES ARE. THERE'S AN ARGUMENT SAYING
22 WELL, IT IMPLIES THAT OR IT INDICATES SUCH, AND IT'S OUR
23 GENERAL POLICY THAT -- I THINK GREATER SPECIFICITY IS, HOW DO
24 WE KNOW THAT? YOU KNOW, THAT THERE WAS A SPECIFIC POLICY ON
25 REVIEWING IT, AND WHAT'S DONE MADE SURE FOLKS, WHEN THEY CHECK

1 THAT BOX YES, DO IT. YOU KNOW, ARE FAMILIAR WITH THAT POLICY
2 AND ARE EXECUTING THAT POLICY.

3 AND THEN I WILL ADJUDGE THIS RULE 17 REQUEST IN THAT
4 LIGHT. I THINK THAT'S THE MOST EFFICIENT WAY TO GO ABOUT THIS.

5 SO I DON'T KNOW, YOU SHOULDN'T NEED TOO MUCH TIME, I WOULD
6 THINK, ANOTHER WEEK, WEEK AND A HALF, TWO WEEKS AT THE MOST TO
7 SUBMIT THE DECLARATION?

8 MR. SPRAGUE: I THINK THAT'S RIGHT, YOUR HONOR.

9 ANOTHER WEEK TO TEN DAYS, I WOULD HOPE THAT WE COULD GET
10 IT IN NEXT WEEK.

11 THE COURT: LET'S SAY END OF NEXT WEEK, THAT'S TEN
12 DAYS ROUGHLY, DOES THAT WORK?

13 MR. SPRAGUE: YES, YOUR HONOR.

14 THE COURT: AND THEN MS. BISCHOF, I WILL GIVE YOU A
15 CHANCE TO COMMENT, NOT RE-BRIEF THE WHOLE THING, BUT IN LIGHT
16 OF WHAT WE JUST SAID, IN LIGHT OF WHAT YOU SEE, IF YOU HAVE
17 FURTHER COMMENT WHY YOU THINK THAT THAT IS NOT SUFFICIENT, I
18 WILL GIVE YOU A WEEK TO FILE YOUR BRIEF.

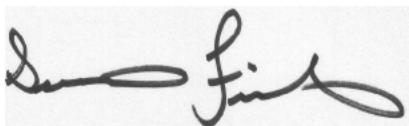
19 MS. BISCHOF: I WILL -- IT IS POSSIBLE, YOUR HONOR,
20 THAT I MAY REQUEST AN EXTENSION. I'M STARTING A TWO AND A HALF
21 WEEK TRIAL ON MAY 15TH. SO IF I -- I WILL SEE IF SOMEONE ELSE
22 IN MY OFFICE CAN WRITE IT IF I CAN'T. I WILL NOT ASK FOR AN
23 EXTENSION UNLESS ABSOLUTELY NECESSARY.

24 THE COURT: OKAY. DO WE HAVE A TRIAL DATE IN THIS
25 CASE?

1
2
3
4 **CERTIFICATE OF REPORTER**
5
6
7

8 I, THE UNDERSIGNED OFFICIAL COURT
9 REPORTER OF THE UNITED STATES DISTRICT COURT FOR
10 THE NORTHERN DISTRICT OF CALIFORNIA, 280 SOUTH
11 FIRST STREET, SAN JOSE, CALIFORNIA, DO HEREBY
12 CERTIFY:

13 THAT THE FOREGOING TRANSCRIPT,
14 CERTIFICATE INCLUSIVE, CONSTITUTES A TRUE, FULL AND
15 CORRECT TRANSCRIPT OF MY SHORTHAND NOTES TAKEN AS
16 SUCH OFFICIAL COURT REPORTER OF THE PROCEEDINGS
17 HEREINBEFORE ENTITLED AND REDUCED BY COMPUTER-AIDED
18 TRANSCRIPTION TO THE BEST OF MY ABILITY.
19
20
21
22

23
24 

25 SUMMER A. FISHER, CSR, CRR
CERTIFICATE NUMBER 13185

DATED: 5/4/23